

CLAIMS

What is claimed is:

- 1 1. A method for performing a cryptographic operation on a message, comprising:
2 (a) generating initial unpredictable information;
3 (b) using said initial unpredictable information, transforming an initial secret
4 quantity into a plurality of randomized quantities having a predetermined
5 logical relationship thereamong; and
6 (c) performing a first step of said operation involving said randomized
7 quantities in a hardware device to reduce the amount of useful information
8 about said operation available from external monitoring of said hardware
9 device.
- 1 2. The method of Claim 1 wherein said initial unpredictable information includes a
2 plurality of random values obtained from a random number generator.
- 1 3. The method of Claim 1 wherein said initial secret quantity includes at least one of
2 the group of secret quantities comprising a message and a key.
- 1 4. The method of Claim 1 wherein step (b) includes a blinding operation.
- 1 5. The method of Claim 4 wherein said blinding operation includes an XOR
2 operation.
- 1 6. The method of Claim 1 wherein the probability that the value of any specific bit in
2 any of said randomized quantities is a "one" is one half (0.5).
- 1 7. The method of Claim 1 wherein step (c) includes separately operating on a
2 plurality of said randomized quantities in a random order.

1 8. The method of Claim 1 wherein said cryptographic operation is compatible with
2 the Data Encryption Standard (DES), said method further comprising
3 recombining the result of step (c) to produce a final result, said final result being a
4 cryptographic representation of said message transformed with said DES
5 algorithm.

1 9. The method of Claim 8 further comprising using said initial unpredictable
2 information to shuffle the S tables.

1 10. The method of Claim 9 wherein said step of using said initial unpredictable
2 information to shuffle said S tables includes blinding the outputs of said S tables.

1 11. The method of Claim 9 wherein said step of using said initial unpredictable
2 information to shuffle said S tables includes permuting said S tables.

1 12. The method of Claim 9 wherein step (c) includes extracting, in random order, data
2 representing the six-bit inputs to the S tables in randomized form from said
3 randomized quantities.

1 13. The method of Claim 1 further comprising:
2 (d) updating at least one of said randomized quantities using additional
3 unpredictable information to generate at least one updated randomized
4 quantity; and
5 (e) performing a second step of said operation involving said at least one
6 updated randomized quantity.

1 14. The method of Claim 13 wherein step (d) includes reordering the bit positions of
2 said at least one randomized quantity.

- 1 15. The method of Claim 13 wherein step (d) includes randomizing the bit values of
2 said at least one randomized quantity.
- 1 16. The method of Claim 13 wherein step (d) includes incrementing and checking a
2 failure counter prior to said updating, and clearing said failure counter following
3 said updating.
- 1 17. The method of Claim 13 wherein step (c) includes performing said first step of
2 said operation using a plurality of parameters, said method further comprises
3 using said initial unpredictable information to initialize said parameters and
4 updating said parameters to generate a plurality of updated parameters, and step
5 (e) includes performing said second step of said operation using said updated
6 parameters.
- 1 18. A method for performing a cryptographic operation on a message using a key,
2 comprising:
3 (a) using unpredictable information, transforming said message into a
4 plurality of message portions having a predetermined logical relationship
5 thereamong;
6 (b) using unpredictable information, transforming said key into a plurality of
7 key portions having a predetermined logical relationship thereamong;
8 (c) performing a first step of said cryptographic operation on said message
9 portions using said key portions in a hardware device to reduce the amount
10 of useful information about said operation available from external
11 monitoring of said hardware device;
12 (d) updating at least one of said plurality of message portions with
13 unpredictable information;
14 (e) updating at least one of said plurality of key portions with unpredictable
15 information;

- 16 (f) performing at least a second step of said cryptographic operation on said
- 17 message portions using said key portions in a hardware device to reduce
- 18 the amount of useful information about said operation available from
- 19 external monitoring of said hardware device; and
- 20 (g) returning a cryptographic result.

1 19. The method of Claim 18 wherein said cryptographic operation is compatible with
 2 the Data Encryption Standard (DES) such that said result is a representation of the
 3 value derived by applying the DES algorithm to said message.

1 20. The method of Claim 18 further comprising a step of using unpredictable
 2 information to reshuffle the S tables between step (c) and step (f).

1 21. The method of Claim 18 wherein said step (b) establishes a predefined
 2 mathematical relationship between said key portions and said secret quantity
 3 which is preserved when said key portions are updated at step (e).

1 22. A cryptographic processing device for performing a cryptographic operation in a
 2 manner resistant to discovery of a secret quantity by external monitoring,
 3 comprising:

- 4 (a) an untrusted input for electrical power, from which the device's power
- 5 consumption can be measured;
- 6 (b) a secure memory containing at least a representation of said secret
- 7 quantity;
- 8 (c) a source of unpredictable information for transforming said secret quantity
- 9 into a plurality of randomized quantities having a predetermined logical
- 10 relationship thereamong;
- 11 (d) an input/output interface;

12 (e) a processor connected to said memory, configured to perform
13 cryptographic transformations on randomized forms of data received via
14 said interface using randomized forms of said secret quantity.

1 23. The device of Claim 22 wherein said device comprises an ISO 7816 compliant
2 smartcard.

1 24. The device of claim 22 wherein said power consumption varies measurably
2 during said cryptographic transformations, but where measurements of said power
3 consumption are not correlated to said secret quantity.

1 25. The device of Claim 22 wherein said source of unpredictable information
2 comprises a random number generator.

1 26. The device of Claim 22 further comprising at least one register for temporarily
2 storing said randomized quantities, wherein the correlation between any single bit
3 of said at least one register and said secret quantity is undetectably small, but
4 where the correlation between a combination of multiple bits of said at least one
5 register and said secret quantity is measurably significant.

1 27. The device of Claim 26 wherein said device is an ISO 7816 compliant smartcard.

1 28. A method for performing a symmetric cryptographic operation using a secret key
2 with resistance to external monitoring attacks, comprising:

- 3 (a) obtaining an input message;
- 4 (b) generating initial unpredictable information;
- 5 (c) combining said key, said message, and said unpredictable information;
- 6 (d) deriving a result, where:
 - 7 (i) said result is a predefined function of said input message and of
 - 8 said key, and

- 9 (ii) said result is independent of said unpredictable information; and
10 (e) producing a response based on said result.

1 29. The method of Claim 28 wherein said cryptographic operation is a predefined
2 block cipher.

1 30. The method of claim 29 wherein said block cipher is the Data Encryption
2 Standard.

1 31. The method of claim 29 wherein all steps are implemented in an ISO 7816-
2 compliant smartcard.

1 32. The method of claim 29 wherein individual no bit manipulated in said step (d) is
2 measurably correlated to any bit of said key.

1 33. A device for performing keyed cryptographic operations, comprising:

- 2 (a) a keyed processing unit, configured to
3 (i) obtain a representation of a secret parameter encoded as a first
4 plurality of parameters,
5 (ii) receive an input datum,
6 (iii) perform a cryptographic operation upon said input datum using
7 said plurality of parameters, and
8 (iv) transmit the result of said cryptographic operation; and
9 (b) a key update unit, configured to
10 (i) obtain said encoded representation of said secret parameter,
11 (ii) obtain a blinding factor,
12 (iii) produce from said first plurality of parameters and said blinding
13 factor a second plurality of parameters where

- 10 (d) deriving a transformed representation of said lookup table from said
11 received lookup table and said unpredictable information;
12 (e) deriving new input and output masking parameters corresponding to said
13 transformed representation of said table;
14 (f) storing said transformed lookup table and said input and output masking
15 parameters in a memory; and
16 (g) using said transformed table in a cryptographic computation.

1 38. The method of claim 37 where step (d) includes the following substeps:

- 2 (a) obtaining a first random value;
3 (b) generating a new output masking value from said first random value and
4 an output masking value received at step (b);
5 (c) obtaining a second random value;
6 (d) generating a new input masking value from said second random value and
7 an input masking value received at step (b);
8 (e) producing said transformed table with the property that the i^{th} element in
9 the transformed table is equal to the result of
10 (i) finding the element at the location in the original table specified by
11 taking an index 'i' XORed with said old input mask,
12 (ii) XORing said element with the values of both said new output
13 mask and said old output mask
14 (iii) storing said XOR result in said transformed table at a location
15 corresponding to said index 'i' XORed with said new input mask

1 39. The method of claim 38 where the steps are performed in a different order.

1 40. A method for transforming data in a smartcard using the Data Encryption
2 Standard with a secret key, comprising the steps of:

- 3 (a) receiving a representation of a message;

4 (b) combining at least a portion of said message representation with at least a
5 portion of a representation of said key to produce a DES intermediate
6 representation;
7 (c) producing from said DES intermediate an index to an S operation, where
8 said index is a representation of a traditional 6-bit S table input;
9 (d) performing an S operation, producing an S result in an expanded
10 representation for which the Hamming Weight of said S result is
11 independent of the value of said S table input;
12 (e) combining the result of said S operation with said DES intermediate to
13 produce a new DES intermediate representation;
14 (f) repeating steps (c) through (e) a plurality of times; and
15 (g) converting the final DES intermediate representation into a DES result,
16 where said DES result is a representation of the result of applying the DES
17 standard to said message with said secret key.